REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

I. DOUBLE PATENTING

The Examiner submits that claims 1-3 of the present application conflict with claims 7, 8 and 9, respectively, of United States Patent Application No. 09/711,323, filed November 9, 2000 by de Jesus Valdes et al (hereinafter the "'323 Application'"). In response, the Applicants have cancelled claims 7, 8 and 9 from the '323 Application. Accordingly, the Applicants respectfully submit that there is no instance of double patenting in relation to the present Application and the '323 Application.

II. REJECTION OF CLAIMS 1-6 UNDER 35 U.S.C. § 103

Claims 1-6 stand rejected as being unpatentable over the Bristol patent (U.S. 6,690,274, issued February 10, 2004, hereinafter "Bristol"). The Applicants respectfully traverse the rejection.

Particularly, the Examiner's attention is directed to the fact that Bristol fails to disclose or suggest the novel invention of organizing alerts into classes by evaluating a similarity between a new alert and an existing class of alerts, including adjusting or updating an expectation that feature values of the new alert and feature values of the existing alert class will match, as claimed in Applicants' independent claims 1, 3, 4, 5 and 6.

Firstly, Bristol fails to teach or even suggest the desirability of adjusting or updating an expectation that feature values of a new alert and feature values of an existing alert class will match. As described in the Applicants' specification, the nature of an alert may affect a similarity expectation that indicates which features (e.g., source IP address, destination IP address, type of attack, etc.) of the alert should be similar to corresponding features of an existing alert class (See, for example, page 6, lines 25-28 and page 7, line 20 – page 9, line 13). For example, if a new alert indicates a SYN flood attack (in which source IP addresses are typically forged), similarity of source IP addresses might not provide a meaningful basis for comparison between the new alert

and an existing alert class. Thus, when comparing the new alert to an existing alert class for correlation purposes, it may be necessary to adjust or update this similarity expectation in order to make a meaningful comparison.

The portion of Bristol that the Examiner cites as allegedly teaching this limitation <u>at most</u> teaches that a group of generated alarms is scanned for alarms that match user-selected criteria (*e.g.*, certain full or partial character patterns). Bristol does not teach, however, that analysis of a given alarm based on the user-selected criteria is <u>adjusted or updated by an expectation that features values the given alarm and the user-defined criteria will match</u>. That is rather than comparing alarms to alarms (*e.g.*, comparing a newly generated alarm to an existing alarm), Bristol, at best, compares existing alarms, individually, to some sort of user-defined search or filtering criteria.

Secondly, Bristol does not teach defining a new alert class if a newly generated alert does not correspond to an existing alert class. This limitation is not addressed by the Examiner's analysis of claims 1-6 in the Office Action. However, Bristol is directed not to a method that seeks to classify each generated alarm, but rather to a method that scans generated alarms for those that exemplify specific desired criteria. Thus, if a given alarm does not exemplify the desired criteria for which the method is scanning, there is no need to treat the given alarm any further (such as by generating a new class of alarms defined by the given alarm).

Notably, Applicants' invention claims a method in which alerts are grouped into classes based on similar feature values, <u>an expectation that feature values of a new alert and feature values of an existing alert class will match is adjusted or updated</u>, and <u>a new alert class is defined if the new alert does not match an existing alert class</u>, as recited by the Applicants in claims 1, 3, 4, 5 and 6. Specifically, Applicants' claims 1, 3, 4, 5 and 6 positively recite:

1.   In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:
    (a) receiving a new alert;
    (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
    (c) updating a minimum similarity requirement for one or more features;

(d) <u>updating a similarity expectation for one or more features;</u>

(e) comparing the new alert with one or more alert classes, and either:

(f1) associating the new alert with the existing alert class that the new alert most closely matches; or

(f2) <u>defining a new alert class that is associated with the new alert</u>. (Emphasis added)

3.   In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value;

(e) <u>adjusting the comparison by an expectation that certain feature values will or will not match</u>, and either:

(f1) associating the new alert with the existing alert class that the new alert most closely matches; or

(f2) <u>defining a new alert class that is associated with the new alert</u>. (Emphasis added)

4.   In an intrusion detection system that includes a plurality of sensors, each of which generates alerts when attacks or anomalous incidents are detected, a method for organizing the alerts comprising the steps of:

(a) receiving an alert;

(b) identifying a set of features that may be shared by the received alert and one or more existing alert classes;

(c) <u>setting a minimum similarity value for one or more features or feature groups;</u> comparing the new alert to one or more of the alert classes, and either:

(d1) <u>defining a new alert class that is associated with the received alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value</u>; or

(d2) associating the received alert with the existing alert class that the received alert most closely matches. (Emphasis added)

5.   In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:

(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or

more existing alert classes;

(c) <u>updating a minimum similarity requirement for one or more features</u>;

(d) comparing the new alert with one or more alert classes, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) <u>defining a new alert class that is associated with the new alert</u>. (Emphasis added)

6. In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) <u>rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value</u>, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) <u>defining a new alert class that is associated with the new alert</u>. (Emphasis added)

As discussed above, nowhere does Bristol teach or even suggest the desirability of <u>adjusting or updating an expectation that feature values of a new alert and feature values of an existing alert class will match is adjusted or updated</u> or <u>defining a new alert class if the new alert does not match an existing alert class</u>. Therefore, the Applicants submit that independent claims 1, 3, 4, 5 and 6 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not made obvious by the teachings of Bristol. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

III. NEW CLAIMS

The Applicants have added new claims 7-30. New claims 7-17 recite the limitations of original claims 1-6 in computer readable medium and system form. New

claims 18-21 comprise cancelled claims 6-9 of the '323 Application, and new claims 22-30 recite claims 18-21 in computer readable medium and system form.
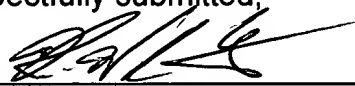
IV. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

_7/11/06_
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702